UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

SOCIÉTÉ DU FIGARO, SAS, *et al.*, Plaintiffs, v. APPLE INC., Defendant.	No. 4:22-cv-04437-YGR (TSH)

JOINT LETTER BRIEF REGARDING PROTECTIVE ORDER

The Honorable Thomas S. Hixson
San Francisco Courthouse
Courtroom B, 15th Floor
450 Golden Gate Avenue
San Francisco, CA 94102

Dear Judge Hixson:

Pursuant to the Court's Discovery Standing Order, plaintiffs Société du Figaro, SAS; L'Équipe 24/24 SAS; and le GESTE (Plaintiffs) and defendant Apple Inc. (Apple) respectfully submit this joint letter brief regarding the form and substance of the protective order to be entered in the above-referenced matter.

At the Court's direction, the parties met and conferred further following the hearing on January 13, 2023. Based on the Court's January 17, 2023 order, and by way of agreeing to a few non-substantive changes, the Parties have narrowed the instant dispute to Apple Inc.'s proposed Sec. 9. Unfortunately, notwithstanding their efforts, the parties have been unable to resolve their dispute, per the below. Therefore, Plaintiffs and Apple submit forms of order that differ only as to the inclusion or not of that proposed Sec. 9. The parties look forward to the hearing scheduled for tomorrow, January 20, 2023, and thank the Court for its assistance in resolving this matter.

DATED: January 19, 2023

HAGENS BERMAN SOBOL SHAPIRO LLP

By: /s/ *Robert F. Lopez*
Robert F. Lopez
Counsel for Plaintiffs

GIBSON DUNN CRUTCHER LLP

By: /s/ *Caeli A. Higney*
Caeli A. Higney
Counsel for Apple Inc.

Plaintiffs' position and final proposed compromise: Plaintiffs respectfully ask the Court to enter their proposed protective order, which is attached as Ex. A. (A redlined comparison is attached as Ex. B, showing differences between it and the protective order (ECF No. 381) on file in the related case *In re Apple iPhone Antitrust Litig.*, N.D. Cal. No. 4:11-cv-06714-YGR-TSH.) Exhibit A reflects Plaintiffs' position and final proposed compromise. (*N.B.*: Apple's section on supposed "concessions" is unfair; *e.g.*, Plaintiffs do *not* concede that Apple *will* suffer harm as posited.)

Further background: On December 23, 2022, Plaintiffs and Apple submitted a joint statement addressing areas of disagreement regarding the protective order to be entered in this case. The Court heard argument on January 13, 2023. On January 17, the Court issued an order in which it ruled on most items in dispute, leaving only the matter of Apple's proposed Sec. 9 to resolve.

During the January 13 hearing, the Court directed the Parties to meet-and-confer further regarding proposed Sec. 9. During a subsequent meet-and-confer on January 17, Apple provided Plaintiffs certain confidential information, and the Parties concluded the session by agreeing to consider Sec. 9 in light of this information and otherwise. Next, on January 18, Apple sent Plaintiffs a revised proposed protective order, which included several revisions to its proposed Sec. 9. At another conference later that day, the Parties again engaged on these matters, including with respect to Apple's new revisions. At the end of the session, the Parties agreed to continue considering each other's positions. Plaintiffs have since agreed to Apple's newest non-substantive proposed revisions, as reflected in their Ex. A. Unfortunately, however, the Parties remain at an impasse regarding Apple's (revised) proposed Sec. 9.

Argument and requested relief: Plaintiffs listened carefully to Apple's recitation regarding the "particular facts" its counsel broached at the January 13 hearing. While Apple offered little detail, the information Apple referenced did not support the proposition that without proposed Sec. 9, Apple *will suffer harm or prejudice* in this matter. Therefore, Apple still has not shown good cause for the extensive and serious changes it seeks. *See, e.g.*, *Corley v. Google, Inc.*, 2016 WL 3421402, at *1 (N.D. Cal. June 22, 2016) ("This court has 'approved' the model protective orders it provides online, and the model order for use in highly sensitive cases contains 'presumptively reasonable conditions' for managing the discovery of highly sensitive materials. . . . A party who unilaterally requests a deviation from the presumptively valid terms of that model order *must show 'specific harm or prejudice' will result* if the court denies the request; otherwise, the party has failed to show good cause. . . .") (citations omitted) (emphasis added). And Apple still offers no legal authority supporting the new terms it seeks to impose. Apple's new reference to Rule 26 is inapposite; the rule does not stretch to encompass Apple's manifold and varied proposed terms. Thus, it does not begin to justify Apple's proposed "unilateral[] . . . deviation[s]," *Corley* at *1, to the N.D. Cal. model order, which is the basis for Plaintiffs' proposed protective order.

Accordingly, Plaintiffs' view remains that the January 21, 2021 protective order (ECF No. 381) in the related *In re Apple iPhone Antitrust Litig.* matter ought to remain the basis for the protective order to be entered here. That order, negotiated by Apple, was based on the Court's tried-and-true model order for matters involving "Highly Sensitive Confidential Information and/or Trade Secrets." Indeed, it already contains accommodations beneficial to Apple (including a provision regarding privileged material purportedly produced out of inadvertence) that Plaintiffs did not seek

to change. Further, the order that Plaintiffs propose (like the model and consumer orders) *already contains the following provision*: "Protected Material must be stored and maintained by a Receiving Party at a location and in a secure manner that ensures that access is limited to the persons authorized under this Order." (Sec. 7.1 to all of the foregoing.) What is more, Plaintiffs have provided Apple with assurances as to that provision.

As for Section 9.1: Apple's proposed Section 9.1 is unnecessary and unworkably vague. Plaintiffs have repeatedly provided Apple assurances that their counsel have security measures in place and that Plaintiffs' document-database vendor complies with at least one security standard referenced by Apple, among other standards. Further, Plaintiffs' proposed order always has included Sec. 7.1, which addresses secure storage and maintenance. There is, therefore, no need for Section 9.1. Additionally, Apple still does not explain when multi-factor authentication must be implemented nor how often that authentication must be renewed. Apple also has not defined the term "encryption," and it remains unclear how this would apply in practice.

As for Section 9.2: This section seeks to impose various obligations on Plaintiffs in the event of a still exceedingly ill-defined "Data Breach." Indeed, "Data Breach" appears to encompass, *inter alia*, inadvertent access by a court reporter to Protected Material on a device before the reporter has executed Exhibit A; inadvertent use by a legal assistant of Protected Material via a device for permitted purposes before the assistant has signed Exhibit A; the e-filing by an assistant of a redacted page of Protected Material on the docket without a sealing motion, where the assistant thought none was required; or a colleague's use without explicit permission of a lawyer's device that has access to Protected Material, despite not accessing any. In short, Apple has not addressed the Court's concern that the language in this section is so vague as to be unworkable. Yet the introduction to this section would impose a requirement that, in the event of a "Data Breach," Plaintiffs must "cooperate" with Apple to satisfy Apple's indeterminate "legal, contractual, or other obligations." Plaintiffs should not be required to undertake obligations that they are not otherwise legally required to bear, particularly where Apple does not even begin to identify these obligations, let alone in detail. Additionally, Apple would require Plaintiffs to "recover" or "protect" materials impacted in the event of a "Data Breach"—even if that "Data Breach" targeted a vendor, over which Plaintiffs do not have control. Plaintiffs should not be required to take on a duty that is beyond their power to perform. Finally, Apple has yet to define the term "device" either as a term or functionally, nor has it explained what is meant by "[m]aterials" that are "potentially subject to" a "Data Breach," further rendering this entire section unworkably vague.

Subsection (a), (b), and (c) of Section 9.2 are similarly unjustified. Subsection (a) would require Plaintiffs to disclose the specifics of their data security systems to Apple, including "underlying vulnerabilities or flaws" with Plaintiffs' systems and the "specific actions" Plaintiffs have taken in response. Such a requirement is not only unduly burdensome and unjustifiably intrusive, but it also creates increased security risks for Plaintiffs' counsel and their firm, even beyond the scope of this case. Furthermore, this section would require Plaintiffs to provide specific details about their vendor's security system, which Plaintiffs are not in a position to do—and which also would create security concerns. Additionally, Apple does not actually explain, let alone persuasively, how this sort of *post hoc* information would help in the aftermath of a breach.

Moreover, proposed terms such as these, which would require meet-and-confers on a litany of topics in the event of a so-called "Data Breach," are inappropriate and wholly unsupported by the

rules or legal precedent. They also are unduly burdensome. Again, Apple defines a "Data Breach" to include situations where there is no reason to believe the Designating Party's Protected Materials are actually involved, *see* Prop. Sec. 9.2 (referring to "devices"). For example, if an unauthorized individual accessed documents on a vendor "device" (an undefined term) in an entirely unrelated case, this does *not* mean that the individual would have access to *Apple's* Protected Materials as well. Nor does Apple define what it means for a Receiving Party to learn that Protected Materials are "potentially subject" to what it would deem a "Data Breach." (*See id.*) Further, it is unclear what it means to "affect[]" Protected Material when a "Data Breach" is defined as merely implicating access to a device, as noted above. In any event, Apple always could ask Plaintiffs that various steps be taken, and if need be, could petition the Court for an order requiring that certain steps be taken, where necessary and appropriate. Then any such matters could be dealt with concretely and appropriately, with particularity.

As for Section 9.3: The Parties' obligations regarding Protected Materials already are set forth in Sec. 7.1 to Plaintiffs' (and Apple's) proposed orders, as in the model order. And, notwithstanding Apple's vague references to "Applicable Data Law," reminders that Parties must follow the law are extraneous and unnecessary in a protective order.

Accordingly, for the reasons Plaintiffs expressed in the Parties' first joint statement, at the January 13 hearing, and in their sections herein, Plaintiffs respectfully ask (a) that the Court decline to order that Apple's Proposed Sec. 9 be included in the order to be entered in this matter; and (b) that their proposed order, at Exhibit A, be entered instead.

Apple's Position: Apple respectfully asks the Court to enter its proposed protective order (Ex. C).

Plaintiffs Concede That Data Should be Protected. Following the Court's January 13, 2023 hearing and January 17, 2023 order (Dkt. 57), Apple has sought in good faith to negotiate with Plaintiffs on appropriate data-security provisions to include in a stipulated protective order. Plaintiffs' counsel do not dispute that Apple will suffer harm if protected materials fall into the hands of malicious actors, or that reasonable data-security measures are warranted; indeed, they have repeatedly stated that their firm and discovery vendor already comply with several of Apple's proposed requirements. For example, they claim that they already use multi-factor authentication, and that their vendor (but not their firm) has an information security management system that complies with one of the industry or government frameworks that Apple cites (*see* Ex. C § 9.1). Nor do Plaintiffs dispute that it is reasonable for a receiving party to notify and reasonably cooperate with a producing party whose protected materials are compromised in a data breach. Plaintiffs simply do not want to be *required* to take these reasonable steps and, therefore, refuse to meaningfully engage with Apple to identify appropriate data-security requirements.

Data-Security Provisions Belong in This Protective Order. In Plaintiffs' view, since cyberattacks cannot be predicted with certainty, data-security provisions do not belong in protective orders *at all*—despite numerous attacks affecting discovery materials. In today's threat environment, data breaches are not speculative and can cause significant harm. It is not unreasonable to have appropriate and specific measures in place to prevent and quickly contain a breach.

There is no question that measures to prevent and remedy a breach of confidential materials constitute protection from expense, burden, annoyance, and embarrassment, *i.e.*, the purpose of a protective order under Rule 26(c)(1). The financial costs of a data breach alone justify requiring reasonable security measures of parties handling protected materials.[1] The model protective order itself includes a line requiring data security: "Protected Material must be stored and maintained by a Receiving Party at a location and in a secure manner that ensures that access is limited to the persons authorized under this Order." Model Stipulated Protective Order (for standard litigation) § 7.1 (N.D. Cal.). But in light of ever-present and growing data-security threats, *see* Dkt. 51 at 4-5, more detailed data-security provisions than provided for by the current model order are necessary. Leaving it to each party independently to decide what security is appropriate, as Plaintiffs' approach provides, ignores findings from authorities like the California Department of Justice that have studied this issue, concluding that one of the security frameworks invoked by Apple represents "*a minimum level* of information security that all organizations that collect or maintain personal information should meet." *See id.* at 4 & n.5. Although Apple is pursuing a much-needed update to the model protective order, hackers are not waiting for that process to complete before targeting law firms and vendors holding sensitive materials. Many litigants are already including specific data-security provisions in recent protective orders.[2]

[1] *See Cost of a Data Breach Report 2022*, IBM Security at 5, tinyurl.com/2s3nmj65 ("Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022.").

[2] *See* Dkt. 51 at 4 n.4; *see also*, *e.g.*, *Martin v. Walmart Inc.*, Case No. 2:22-cv-01832-JLS-E (C.D. Cal. Aug. 25, 2022) (Dkt. 28, § 5.5); *Maldonado v. DSV Solutions*, Case No. 5:21-cv-01594-GW-SP (C.D. Cal. May 12, 2022) (Dkt. 15, § 5.5); *Frasco v. Flo Health, Inc.*, Case No. 3:21-cv-00757-

Apple Has Proposed Reasonable Changes to its Proposed Data-Security Provisions. Apple's proposed data-security provisions incorporate industry standards and widely recognized best practices. Seeking to accommodate Plaintiffs, Apple has revised its proposal, at this time seeking what should be *minimal* guarantees. *See* Ex. D (Redline).

Encryption. Electronic transfer of sensitive data without encryption is not secure.[3] In light of the Court's questions around the meaning of "transit" and the administrability of encryption requirements, Apple now proposes clarifying language. Apple submits that, "where reasonably practical," a party should encrypt protected materials at rest and "in electronic transit outside of network(s) covered by the Party's information security management system."[4] Ex. C § 9.1. Similar provisions appear in protective orders with data-security provisions.[5]

Multi-factor Authentication. Apple has proposed requiring multi-factor authentication ("MFA") for access to protected materials. To avoid any confusion, Apple has incorporated the definition of MFA used by the National Institute of Standards and Technology (a federal agency that promotes U.S. innovation and industrial competitiveness). *Id.* § 9.1 n.1. This requirement would be satisfied, for example, if persons must use a recognized device *and* enter a password for access to a database with protected materials. Using passwords alone leaves materials vulnerable to attack, but MFA is a low-burden, highly effective security mechanism that Americans use every day (more often than they even realize).[6] Indeed, the federal judiciary requested congressional

---

JD (N.D. Cal. Jan. 11, 2022) (Dkt. 112, § 12.10) *Diaz v. Google LLC*, Case No. 5:21-cv-03080-NC (N.D. Cal. Oct. 12, 2021) (Dkt. 50, § 14.9); *Cruz v. WalMart Inc.*, Case No. 2:21-cv-00613-WBS-CKD (E.D. Cal. Sept. 3, 2021) (Dkt. 16, § 6); *Cervantes v. Wal-Mart Stores, East, LP*, Case No. 1:21-cv-00750-CMA-NYW (D. Colo. June 29, 2021) (Dkt. 27, § 6); *Klaustech LLC v. Google LLC*, Case No. 4:20-cv-04459-JSW (N.D. Cal. June 24, 2021) (Dkt. 52, § 14.11).

[3] *See Data Protection: Data In transit vs. Data At Rest*, DataInsider (Digital Guardian's Blog) (Nov. 28, 2022), tinyurl.com/t9kjat27 ("Unprotected data, whether in transit or at rest, leaves enterprises vulnerable to attack . . . . [O]ne of the most effective data protection methods for both data in transit and data at rest is data encryption."); David G. Ries, *2021 Cybersecurity*, American Bar Association (Dec. 21, 2021), tinyurl.com/5n6znc8h (suggesting that employing encryption is an ethical obligation for attorneys).

[4] *See Data In transit*, *supra* n.3 ("For protecting data in transit, enterprises often choose to encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc) to protect the contents of data in transit. For protecting data at rest, enterprises can simply encrypt sensitive files prior to storing them and/or choose to encrypt the storage drive itself.").

[5] *See*, *e.g.*, *Martin v. Walmart*, *supra* n.2 ("Adequate security . . . includes . . . data encryption in transit, data encryption at rest, data access controls, and physical security[.]").

[6] *See Multifactor Authentication*, Cybersecurity & Infrastructure Security Agency, cisa.gov/mfa ("Malicious cyber actors are increasingly capable of phishing or harvesting passwords to gain unauthorized access."); *What is: Multifactor Authentication*, Microsoft Support, tinyurl.com/385mkaat ("Almost every online service from your bank, to your personal email, to your social media accounts supports adding a second step of authentication . . . .").

funding to implement enterprise-wide multi-factor authentication this fiscal year.[7]

Ambiguities. To alleviate concerns about any ambiguities in the proposed provisions, Apple proposes including a mechanism for the parties to resolve questions over compliance with the protective order's data-security provisions. *Id.* § 9.1(c). As with its entire proposal, Apple's goal is to facilitate the parties' collaboration in ensuring that protected data is secure.

Notification and Reasonable Cooperation Following a Breach. Prompt notification and reasonable cooperation are vital to mitigate the consequences of a data breach.[8] Instead of agreeing to a set plan so that the parties can start working together to investigate and contain a data breach in the most critical time to mitigate damage, Plaintiffs suggest that it is only *after* a party realizes that protected materials have been compromised that the parties should decide how to move forward. Even worse, Plaintiffs also suggest that collaborative investigation is unnecessary, evincing a lack of understanding that data breaches often require weeks if not months to contain. Apple has revised its proposal so that notification and other post-breach obligations will only apply after actual breaches—not merely suspected breaches. *Id.* § 9.2. Finally, under Apple's proposal, a receiving party would need to provide a copy of its security policies and procedures for protected materials *only* in the event of a breach affecting the producing party's protected material—a measure that will facilitate cooperation and investigation of a data breach. *Id.* § 9.2(c).

[7] *See The Judiciary Fiscal Year 2023 Congressional Budget Request: Judiciary Information Technology Fund*, The Administrative Office of the U.S. Courts (Mar. 2022), tinyurl.com/32ruwm6w.

[8] For example, in its proposed rule on Cybersecurity Risk Management, the SEC would call for notice of significant cybersecurity incidents "promptly, but in no event more than 48 hours, after having a reasonable basis to conclude" that an incident "occurred or is occurring." 87 Fed. Reg. 13,524, 13, 592 (proposed Mar. 9, 2022) (to be codified at 17 C.F.R. § 275.204-6); *see also*, *e.g.*, *Anderson v. Gen. Motors, LLC*, Case No. 2:22-cv-00353-KJM-DMC (E.D. Cal. Sept. 6, 2022) (Dkt. 38, § 29) ("If a Receiving Party or Authorized Recipient discovers any . . . breach of security [it shall] immediately provide written notice to the Producing or Designating Party of such breach . . . . The Receiving Party or Authorized Recipient agrees to cooperate with the Producing or Designating Party or law enforcement in investigating any such security incident.").

ECF SIGNATURE ATTESTATION

In accordance with Local Rule 5-1, the filer of this document hereby attests that the concurrence of the filing of this document has been obtained from the other signatories hereto.

Dated: January 19, 2023

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Caeli A. Higney*
Caeli A. Higney

Attorneys for defendant Apple Inc.